CLAIMS

What is claimed is:

1.   An apparatus, comprising:

at least one reconfigurable processing device;

at least one authentication processing device; and

at least one interface processing device to be coupled to at least one of said

reconfigurable processing device and said authentication processing device;

wherein the apparatus is adapted to forward information to configure at least one

of said reconfigurable processing device and said interface processing device, received by

said apparatus, to said authentication processing device to verify that the information

came from an authorized source.

2.   The apparatus according to Claim 1, wherein said interface processing device

comprises at least one of a data firewall and a configuration firewall.

3.   The apparatus according to Claim 2, wherein said interface processing device

includes one or more data node registers to configure said data firewall to permit

forwarding of data to at least one of said at least one reconfigurable processing device.

4.   A system, comprising:

at least one reconfigurable processing device;

at least one authentication processing device;

at least one interface processing device to be coupled to at least one of said

reconfigurable processing device and said authentication processing device;

at least one analog front-end device to be coupled to at least one of said at least

one reconfigurable processing device; and

an antenna selected from the group consisting of monopole antennas, dipole

antennas, antenna arrays, loop antennas, planar antennas, and reflector-type antennas.

wherein the system is adapted to forward information to configure at least one of

said reconfigurable processing device and said interface processing device, received by

the system, to said authentication processing device to verify that the information came

from an authorized source.

5.   The system according to Claim 4, further comprising:

at least one host device to be coupled to said at least one interface processing

device, the at least one host device adapted to provide information to be processed by at

least one of said at least one reconfigurable processing device.

6.   The system according to Claim 4, further comprising:

at least one analog front-end interface device to couple between at least one of

said at least one reconfigurable processing device and said at least one analog front-end

device.

7.   A method, comprising:

processing received information with a processing device specified by said

received information if said received information comprises data and if the processing

device is authorized to process said received information; and

performing an authentication process on said received information if said received

information does not comprise data for transmission.

8.   The method according to Claim 7, wherein said performing an authentication

process comprises:

forwarding said received information to an authentication device if said received

information comprises a request to authorize one or more processing devices to process

received information.

9.   The method according to Claim 8, wherein said performing an authentication

process further comprises:

forwarding at least a portion of said received information to a received

information interface device; and

configuring said received information interface device based at least in part on

said at least a portion of said received information.

10.   The method according to Claim 7, wherein said performing an authentication

process comprises:

verifying that said received information is addressed to an authentication

processing device if said received information comprises processing device configuration

information; and

taking security measures if said received information is not addressed to an

authentication processing device.

11.   The method according to Claim 10, wherein said taking security measures

comprises:

re-addressing said received information to an authentication processing device.

12.   The method according to Claim 10, wherein said taking security measures

comprises at least one of discarding said received information or performing a reset

operation.

13.   The method according to Claim 7, wherein, if said received information

comprises processing device configuration information, said performing an

authentication process comprises:

verifying a primary signature included in said received information; and

verifying a link signature included in said received information if said primary

signature is valid.

14.   The method according to Claim 13, further comprising:

forwarding at least a portion of said received information to an intended

processing device if said link signature is valid; and

using said at least a portion of said received information to configure said

intended processing device.

15. A machine-accessible medium containing software code, which, when executed

by a computing platform, causes said computing platform to perform a method

comprising:

processing received information with a processing device specified by said

received information if said received information comprises data and if the processing

device is authorized to process said received information; and

performing an authentication process on said received information if said received

information does not comprise data for transmission.

16. The machine-accessible medium according to Claim 15, wherein said performing

an authentication process comprises:

forwarding said received information to an authentication device if said received

information comprises a request to authorize one or more processing devices to process

received information.

17. The machine-accessible medium according to Claim 16, wherein said performing

an authentication process further comprises:

forwarding at least a portion of said received information to a received

information interface device; and

configuring said received information interface device based at least in part on

said at least a portion of said received information.

18.   The machine-accessible medium according to Claim 15, wherein said performing

an authentication process comprises:

verifying that said received information is addressed to an authentication

processing device if said received information comprises processing device configuration

information; and

taking security measures if said received information is not addressed to an

authentication processing device.

19.   The machine-accessible medium according to Claim 18, wherein said taking

security measures comprises:

re-addressing said received information to an authentication processing device.

20.   The machine-accessible medium according to Claim 18, wherein said taking

security measures comprises at least one of discarding said received information or

performing a reset operation.

21.   The machine-accessible medium according to Claim 15, wherein, if said received

information comprises processing device configuration information, said performing an

authentication process comprises:

verifying a primary signature included in said received information; and

verifying a link signature included in said received information if said primary

signature is valid.

22.   The machine-accessible medium according to Claim 21, further comprising

software code that, when executed by said at least one computing platform, causes said at

least one computing platform to further perform:

forwarding at least a portion of said received information to an intended

processing device if said link signature is valid; and

using said at least a portion of said received information to configure said

intended processing device.